

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Commissioner
US Department of Commerce
United States Patent and Trademark
Office, PCT
2011 South Clark Place Room
CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE
in its capacity as elected Office

Date of mailing (day/month/year)
28 March 2001 (28.03.01)

International application No.
PCT/EP00/06387

Applicant's or agent's file reference
P99075WO.1P

International filing date (day/month/year)
06 July 2000 (06.07.00)

Priority date (day/month/year)
27 July 1999 (27.07.99)

Applicant

SCHWENK, Jörg

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:
11 January 2001 (11.01.01)

☐ in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was

☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer

Olivia TEFY

Telephone No.: (41-22) 338.83.38

THIS PAGE BLANK (USPTO)

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
1. Februar 2001 (01.02.2001)

PCT

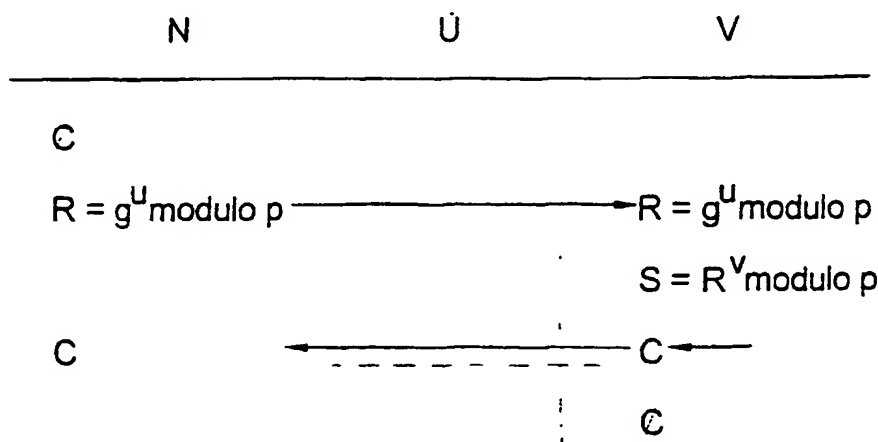
(10) Internationale Veröffentlichungsnummer
WO 01/08347 A1

- (51) Internationale Patentklassifikation⁷: **H04L 9/08** (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): **DEUTSCHE TELEKOM AG** [DE/DE]; Friedrich-Ebert-Allee 140, D-53113 Bonn (DE).
- (21) Internationales Aktenzeichen: **PCT/EP00/06387**
- (22) Internationales Anmeldedatum: **6. Juli 2000 (06.07.2000)** (72) Erfinder; und (75) Erfinder/Anmelder (nur für US): **SCHWENK, Jörg** [DE/DE]; Südwestring 27, D-64807 Dieburg (DE).
- (25) Einreichungssprache: **Deutsch** (74) Gemeinsamer Vertreter: **DEUTSCHE TELEKOM AG**; Rechtsabteilung (Patente) PA1, D-64307 Darmstadt (DE).
- (26) Veröffentlichungssprache: **Deutsch** (81) Bestimmungsstaaten (national): **AU, CA, US.**
- (30) Angaben zur Priorität: **199 35 285.2** 27. Juli 1999 (27.07.1999) **DE** (84) Bestimmungsstaaten (regional): **europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).**

[Fortsetzung auf der nächsten Seite]

(54) Title: **METHOD FOR GENERATING/REGENERATING A CIPHER KEY FOR A CRYPTOGRAPHIC METHOD**

(54) Bezeichnung: **VERFAHREN ZUR GENERIERUNG/REGENERIERUNG EINES CHIFFRIERSCHLÜSSELS FÜR EIN KRYPTOGRAPHIEVERFAHREN**



(57) Abstract: The invention relates to a method for generating/regenerating a cipher key for a cryptographic method, whereby a cipher key and a public key are created from a random number (seed) according to a predetermined deterministic method. According to said method, the seed is created only on the user side through the use of values which are only known to the user. Regeneration information appropriate to the seed regeneration, which allows for the seed to be derived in a deterministic manner from the confidence station through a combination with information known only to said confidence station, is created on the user side and stored in a lossproof manner. In the event of loss of the cipher key, the seed is reproduced on the confidence station side by combining the regeneration information with secrete information.

(57) Zusammenfassung: Bei einem Verfahren zur Generierung/Regenerierung eines Chiffrierschlüssels für ein Kryptographieverfahren, wobei der Chiffrierschlüssel sowie ein öffentlicher Schlüssel mittels eines vorgegebenen deterministischen Verfahrens aus einer großen Zufallszahl (Seed) erzeugt wird, wird der Seed nur nutzerseitig durch Hinzuziehung von nur dem Nutzer bekannten Größen erzeugt. Eine zur Regenerierung des Seeds geeignete Regenerierungsinformation, aus welcher

[Fortsetzung auf der nächsten Seite]

WO 01/08347 A1



Veröffentlicht:

- Mit internationalem Recherchenbericht.
- Vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen.

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

Verfahren zur Generierung/Regenerierung eines Chiffrierschlüssels für ein Kryptographieverfahren

Die Erfindung betrifft ein Verfahren zur Generierung/Regenerierung eines
5 Chiffrierschlüssels für ein Kryptographieverfahren, wobei der Chiffrierschlüssel
sowie ein öffentlicher Schlüssel mittels eines vorgegebenen deterministischen
Verfahrens aus einer großen Zufallszahl (Seed) erzeugt wird.

Zur Sicherung von Kommunikationsdaten und gespeicherten Daten wird immer
10 häufiger die kryptographische Technik der Verschlüsselung eingesetzt. Dabei
werden die Daten unter der Kontrolle eines kryptographischen Schlüssels
chiffriert. Die Daten können mit demselben Schlüssel auch wieder dechiffriert
werden. Marktfähige Produkte und Softwarebibliotheken dazu stehen zur
Verfügung.

15

Meist wird zur Verschlüsselung ein sogenanntes hybrides Verfahren eingesetzt.
Bei diesen Verfahren wird die eigentliche Nachricht mit einem zufällig gewählten
symmetrischen Schlüssel (Session-Key) und einem vorgegebenen symmetrischen
Verschlüsselungsverfahren (z.B. DES, IDEA) verschlüsselt. Der Session-Key wird
20 jeweils mit dem öffentlichen Schlüssel des Empfängers (es sind mehrere
Empfänger möglich) und einem vorgegebenen asymmetrischen oder Public-Key-
Verfahren (z.B. RSA, ElGamal) verschlüsselt. Für jeden Empfänger wird der so
verschlüsselte Session-Key der verschlüsselten Nachricht beigefügt. Eine
Beschreibung dieser Vorgehensweise und der verwendeten Algorithmen findet
25 man z.B. in William Stallings: "Cryptography and Network Security: Principles and
Practice", Prentice Hall, Upper Saddle River, New Jersey, 1998.

Um eine empfangene Nachricht zu entschlüsseln, muß der Empfänger zunächst
mit seinem, zu seinem öffentlichen Schlüssel gehörenden, privaten Schlüssel und
30 dem vorgegebenen Public-Key-Algorithmus den Session-Key entschlüsseln und
dann mit diesem Session-Key die Nachricht entschlüsseln.

Neben der Verschlüsselung von Nachrichten werden kryptographische Verfahren auch zur Verschlüsselung gespeicherter Daten, z.B. auf dem eigenen Personalcomputer, eingesetzt. Auch hier setzt man in der Regel ein hybrides

5 Verfahren ein, bei dem der Nutzer die Daten zunächst mit einem zufällig gewählten symmetrischen Schlüssel (Session-Key) und einem vorgegebenen symmetrischen Verschlüsselungsverfahren (z.B. DES, IDEA) verschlüsselt. Der Session-Key wird dann wiederum mit dem öffentlichen Schlüssel des Nutzers und einem vorgegebenen asymmetrischen oder Public-Key-Verfahren (z.B. RSA,

10 ElGamal) verschlüsselt.

Der Benutzer entschlüsselt zunächst mit seinem, zu seinem öffentlichen Schlüssel gehörenden, privaten Schlüssel und dem vorgegebenen Public-Key-Algorithmus den Session-Key und dann mit diesem Session-Key die gespeicherten Daten.

15

Der jeweils private Schlüssel des Benutzers bzw. des Empfängers ist im folgenden mit dem Begriff Chiffrierschlüssel bezeichnet.

Der Chiffrierschlüssel wird entweder auf einer Chipkarte gespeichert, wobei der

20 Zugriff auf die Chipkarte durch eine nur dem Benutzer bekannte Geheimzahl (PIN) geschützt ist, oder er wird auf einem anderen Speichermedium (z.B. Festplatte oder Diskette) gespeichert, wobei er durch ein möglichst langes Paßwort geschützt wird.

25 Der Chiffrierschlüssel kann verloren gehen. Wenn beispielsweise das Speichermedium zerstört wurde, auf dem er sich befand, oder wenn der Nutzer die PIN oder das Paßwort vergessen hat, mit dem der Chiffrierschlüssel gesichert war, ist ein Zugriff auf chiffrierte Daten damit nicht mehr möglich.

30 Um bei einem Verlust des Chiffrierschlüssels chiffrierte Daten wieder zugänglich machen zu können, sind Mechanismen notwendig, um den Chiffrierschlüssel auf

sichere Weise regenerieren zu können. Zu diesem Zweck wird heute in der Regel der Chiffrierschlüssel an einer zentralen Vertrauensstelle erzeugt und sicher aufbewahrt. Die Erzeugung des Chiffrierschlüssels erfolgt in der Regel dadurch, daß zunächst mit einem statistisch guten Zufallsprozeß eine große Zufallszahl (Seed) erzeugt wird. Aus dieser Zufallszahl wird dann mit Hilfe eines deterministischen Verfahrens das Schlüsselpaar öffentlicher Schlüssel/privater Schlüssel erzeugt. Der Seed wird anschließend gelöscht. Der Nutzer erhält eine Kopie seines Chiffrierschlüssels zur Benutzung zugestellt.

- 10 Der Nutzer hat dabei keinen Einfluß auf die Erzeugung und Aufbewahrung seines Chiffrierschlüssels. Ferner ist es aufwendig, den erzeugten Chiffrierschlüssel sicher zum Nutzer zu transportieren. Als Transportmedium dient heutzutage beispielsweise die oben erwähnte Chipkarte, die dem Nutzer zugesendet wird. Auch ist ein Mißbrauch des gespeicherten Schlüssels durch die Vertrauensstelle oder ein Bekanntwerden des eigenen Schlüssels durch eine Fehlfunktion der Vertrauensstelle bei der beschriebenen Vorgehensweise nicht auszuschließen.

Aufgabe der vorliegenden Erfindung ist es, ein Verfahren der eingangs genannten Art anzugeben, welches die oben angeführten Probleme löst. Insbesondere soll das Verfahren dem Benutzer allein die Entscheidung überlassen, ob ein Schlüssel wiederhergestellt werden soll.

- Dem zur Lösung der Aufgabe hier vorgeschlagenen Verfahren liegt der Gedanke zugrunde, daß eine Hinterlegung des Chiffrierschlüssels zu Sicherheitszwecken bei der Vertrauensstelle entfallen kann, wenn der Seed (S) nur nutzerseitig durch Hinzuziehung von nur dem Nutzer bekannten Größen (u) erzeugt wird, daß eine zur Regenerierung des Seeds geeignete Regenerierinformation (R), aus welcher der Seed von der Vertrauensstelle durch Verknüpfung mit nur ihr bekannten Informationen (v) deterministisch ableitbar ist, nutzerseitig erzeugt und verlustsicher aufbewahrt wird und daß im Falle eines Verlustes des Chiffrierschlüssels (C) durch Verknüpfung der Regenerierinformation (R) mit den

geheimen Informationen (v) der Seed (S) seitens der Vertrauensstelle wieder hergestellt wird.

Dies kann bei einer ersten Ausgestaltung der Erfindung dadurch verwirklicht

5 werden, daß eine mathematische Abbildung (Schlüsselvereinbarungsabbildung) k : $k(x,y)=z$ vorgesehen ist, für die gilt:

a) $k(k(u,v),w) = k(k(u,w),v)$ für alle u,v,w ,

b) aus der Kenntnis von u und $k(u,v)$ kann in der Praxis nicht auf v geschlossen werden,

10 c) aus der Kenntnis von u , $k(u,v)$ und $k(u,w)$ kann in der Praxis nicht auf $k(k(u,w),v)$ geschlossen werden,

daß ein der Vertrauensstelle bekannter öffentlicher Parameter g und ein seitens der Vertrauensstelle vorhandener geheimer Schlüssel v zu einem öffentlichen Schlüssel $V=k(g,v)$ der Vertrauensstelle verknüpft sind,

15 daß der öffentliche Schlüssel V und eine nutzerseitig gewählte Zufallszahl u nutzerseitig zu dem Seed $S=k(V,u)$ verknüpft werden,

daß aus dem Seed S nutzerseitig durch das vorgegebene deterministische Verfahren das Schlüsselpaar aus Chiffrierschlüssel C und öffentlichem Nutzerschlüssel U abgeleitet wird und

20 daß zur Ermöglichung der Wiederherstellung dieses Schlüsselpaares U und C die Regenerierinformation $R=k(g,u)$ nutzerseitig erzeugt und verlustsicher aufbewahrt wird.

Die Zufallszahl u und der Seed S sollen nach der Erzeugung der

25 Regenerierinformation R zur Sicherheit wieder vernichtet werden. Die Erzeugung der Regenerierinformation R erfolgt unter abhörsicheren Bedingungen, beispielsweise innerhalb des nutzerseitigen Computerterminals, so daß weder die Zufallszahl u , noch der Seed S an die Öffentlichkeit gelangen können. Die

Regenerierinformation R allein ist ohne Kenntnis des geheimen Schlüssels v zur

30 Dechiffrierung von Nachrichten und Daten ungeeignet und muß daher nicht geheim gehalten werden.

Die Regenerierinformation R kann an beliebigem Ort (beispielsweise auf Papier) aufbewahrt und im Bedarfsfall auf beliebigem, abhörbarem Wege (Post, E-Mail, WWW, ftp ...) zu der Vertrauensstelle gesendet werden.

- 5 Beispiele für geeignete Schlüsselvereinbarungsabbildungen k sind bekannt aus der Zahlentheorie. Beispielsweise kann vorgesehen sein, daß die Schlüsselvereinbarungsabbildung k eine diskrete Exponentialfunktion modulo einer großen Primzahl p: $k(x,y) := x^y \text{ modulo } p$ ist und daß der öffentliche Parameter g ein Element eines mathematischen Körpers $GF(p)$ von großer
- 10 multiplikativer Ordnung ist, oder daß die Schlüsselvereinbarungsabbildung k die Multiplikation auf einer elliptischen Kurve ist. Die Größenordnung der verwendeten Zahlen ist in der Praxis so zu wählen, daß es auch unter Aufbietung moderner technischer Mittel nicht möglich ist, den Wert y aus den Werten x und $k(x,y)$ zu errechnen, was unter Voraussetzung heutiger Dechiffriertechnik bei
- 15 Größenordnungen der verwendeten Primzahlen zwischen 500 und 1000 Bit gewährleistet ist.

Eine Beschreibung derartiger Funktionen findet man in William Stallings:

- "Cryptography and Network Security: Principles and Practice", Prentice Hall, Upper
- 20 Saddle River, New Jersey, 1998. Die vorliegende Erfindung benutzt das Prinzip des Diffie-Hellman-Schlüsselaustausches, der ebenfalls in dem genannten Werk beschrieben wird. Bei dem erfindungsgemäßen Verfahren wird aber, wie oben beschrieben, eine Vertrauensstelle vorausgesetzt, die bei Bedarf den Chiffrierschlüssel C mit Hilfe der Regenerierinformation R wieder herstellen kann.

25

Es kann zur weiteren Ausgestaltung der Erfindung vorgesehen sein, daß zur Wiederherstellung des Chiffrierschlüssels C im Verlustfalle seitens der Vertrauensstelle aus der Regenerierinformation R der Seed $S=k(R,v)$ berechnet wird. Aus dem so rekonstruierten Seed S ist dann über das deterministische

- 30 Verfahren der verlorene Chiffrierschlüssel C selbst berechenbar.

Aufgrund der Eigenschaft der verwendeten Abbildung k gilt $k(R,v) = k(k(g,u),v)$
 $= k(k(g,v),u) = k(V,u) = S$, was tatsächlich wieder dem ursprünglichen Seed S

entspricht. Da der Vertrauensstelle das deterministische Verfahren ebenfalls
bekannt ist, kann der Chiffrierschlüssel C mit Hilfe der Regenerierinformation R

- 5 sehr leicht von der Vertrauensstelle auch ohne Kenntnis der Zufallszahl u wieder
hergestellt werden. Der regenerierte Chiffrierschlüssel C muß dem Nutzer dann
auf abhörsicherem Wege zugestellt werden.

Um einem Mißbrauch des erfindungsgemäßen Verfahrens zur Erlangung fremder

- 10 privater Chiffrierschlüssel C vorzubeugen, kann ferner vorgesehen sein, daß die
Vertrauensstelle nach Berechnung des Seeds S und nach Ableitung des neuen
öffentlichen Nutzerschlüssels U des Nutzers und des neuen Chiffrierschlüssels C
aufgrund eines Schlüsselverlustes überprüft, ob der neu berechnete öffentliche
Schlüssel U mit dem ursprünglichen öffentlichen Schlüssel U des Nutzers

- 15 identisch ist, und den rekonstruierten Chiffrierschlüssel C nur dann an den Nutzer
aushändigt, wenn dies zutrifft. Ein Verfahren zur sicheren Verknüpfung der
Identität des Nutzers mit seinem öffentlichen Schlüssel U ist aus dem
ITU-Standard X.509 bekannt.

- 20 In einer weiteren Ausprägung des Verfahren ist vorgesehen, daß es mehrere
Vertrauensstellen gibt, welche die Schlüsselvereinbarungsabbildung k und den
öffentlichen Parameter g benutzen. Bei der Generierung des Chiffrierschlüssels C
werden eine oder mehrere dieser Vertrauensstellen ausgewählt, wobei mit Hilfe
jeder der ausgewählten Vertrauensstellen ein anderer Teilwert S_v des Seeds

- 25 nutzerseitig wie beschrieben erstellt und die Teilseeds S_v nutzerseitig zu dem
Seed S verknüpft werden. Zur Regenerierung des Chiffrierschlüssels C im
Verlustfalle wird von den ausgewählten Vertrauensstellen ihr jeweiliger Teilwert S_v
des Seeds S mittels der Regenerierinformation R berechnet. Die rekonstruierten
Teilwerte S_v werden zur Rekonstruktion des Chiffrierschlüssels C miteinander zu

- 30 dem Seed S verknüpft. Diese Vorgehensweise kann den Mißbrauch des

Verfahrens durch eine Vertrauensstelle verhindern, da jede Vertrauensstelle nur einen für sich allein unbrauchbaren Teilseed Sv erstellen kann.

In einer weiteren Ausprägung des Verfahrens ist vorgesehen, daß die
5 verschiedenen Vertrauensstellen verschiedene Funktionen kv oder/und
verschiedene öffentliche Parameter gv benutzen und daß für jede der
ausgewählten Vertrauensstellen eine eigene Regenerierinformation Rv erstellt
wird. In diesem Fall muß der Nutzer für jede Vertrauensstelle das
erfindungsgemäße Verfahren durchführen, und von jeder Vertrauensstelle muß ihr
10 jeweiliger Teilseed Sv mit ihrer spezifischen Regenerierinformation Rv erzeugt
werden.

Ausführungsbeispiele der Erfindung sind in der Zeichnung anhand mehrerer
Figuren dargestellt und in der nachfolgenden Beschreibung näher erläutert. Es
15 zeigt:

Fig. 1 ein Ablaufdiagramm der Erzeugung eines nutzereigenen Schlüsselpaares
und

20 Fig. 2 ein Ablaufdiagramm der Rekonstruktion des Chiffrierschlüssels nach
Verlust.

Gleiche Teile sind in den Figuren mit gleichen Bezugszeichen versehen.

25 Fig. 1 zeigt ein zeitliches Ablaufdiagramm der Vorgänge, die zur Erzeugung eines
rekonstruierbaren nutzerspezifischen Chiffrierschlüssels C und eines öffentlichen
Nutzerschlüssels U nach dem erfindungsgemäßen Verfahren notwendig sind. In
der mit N bezeichneten Spalte sind von oben nach unten die nacheinander
auftretenden nutzerseitigen Daten aufgeführt. Ü bezeichnet die
30 Datenübertragungsstrecke zu einer Vertrauensstelle V. Die Vertrauensstelle V
und der Nutzer N verfügen über den öffentlichen Parameter g und die große

Primzahl p . Von der Vertrauensstelle V wird der öffentliche Schlüssel $V = g^v$ modulo p erzeugt und auf einfachem Wege zum Nutzer N übertragen. Der Nutzer erzeugt daraufhin mit einer von ihm gewählten Zufallszahl u einen Seed S und eine Regenerierinformation R und löscht die Zufallszahl u aus Sicherheitsgründen
5 wieder. Die Regenerierinformation G wird an die Vertrauensstelle V übermittelt. Aus dem Seed S wird durch Anwendung eines vorgegebenen und dem Nutzer und der Vertrauensstelle bekannten deterministischen Verfahrens ein öffentlicher Nutzerschlüssel U sowie ein privater, ebenfalls nutzerspezifischer Chiffrierschlüssel C erzeugt. Der Chiffrierschlüssel C dient hier zum Entschlüsseln
10 von Nachrichten oder Daten des Nutzers.

Im Falle eines Verlustes des Chiffrierschlüssels erzeugt die Vertrauensstelle, wie in Fig. 2 gezeigt, den Seed S und den Chiffrierschlüssel C aus der vom Nutzer an die Vertrauensstelle übertragenen Regenerierinformation R durch Verknüpfung
15 mit dem geheimen Schlüssel v neu und übermittelt ihn auf sicherem Wege an den Nutzer.

Patentansprüche

1. Verfahren zur Generierung/Regenerierung eines Chiffrierschlüssels für ein Kryptographieverfahren, wobei der Chiffrierschlüssel sowie ein öffentlicher Schlüssel mittels eines vorgegebenen deterministischen Verfahrens aus einer großen Zufallszahl (Seed) erzeugt wird, **dadurch gekennzeichnet**, daß der Seed (S) nur nutzerseitig durch Hinzuziehung von nur dem Nutzer bekannten Größen (u) erzeugt wird, daß eine zur Regenerierung des Seeds geeignete Regenerierinformation (R), aus welcher der Seed von der Vertrauensstelle durch Verknüpfung mit nur ihr bekannten Informationen (v) deterministisch ableitbar ist, nutzerseitig erzeugt und verlustsicher aufbewahrt wird und daß im Falle eines Verlustes des Chiffrierschlüssels (C) durch Verknüpfung der Regenerierinformation (R) mit den geheimen Informationen (v) der Seed (S) seitens der Vertrauensstelle wieder hergestellt wird.
2. Verfahren nach Anspruch 1 dadurch gekennzeichnet, daß eine mathematische Abbildung (Schlüsselvereinbarungsabbildung) $k: k(x,y)=z$ vorgesehen ist, für die gilt:
 - a) $k(k(u,v),w) = k(k(u,w),v)$ für alle u,v,w ,
 - b) aus der Kenntnis von u und $k(u,v)$ kann in der Praxis nicht auf v geschlossen werden,
 - c) aus der Kenntnis von u , $k(u,v)$ und $k(u,w)$ kann in der Praxis nicht auf $k(k(u,w),v)$ geschlossen werden,.daß ein der Vertrauensstelle bekannter öffentlicher Parameter g und ein seitens der Vertrauensstelle vorhandener geheimer Schlüssel v zu einem öffentlichen Schlüssel $V=k(g,v)$ der Vertrauensstelle verknüpft sind, daß der öffentliche Schlüssel V und eine nutzerseitig gewählte Zufallszahl u nutzerseitig zu dem Seed $S=k(V,u)$ verknüpft werden, daß aus dem Seed S nutzerseitig durch das vorgegebene deterministische Verfahren das Schlüsselpaar aus Chiffrierschlüssel C und öffentlichem Nutzerschlüssel U abgeleitet wird und daß zur Ermöglichung der Wiederherstellung dieses

Schlüsselpaars U und C die Regenerierinformation $R=k(g,u)$ nutzerseitig erzeugt und verlustsicher aufbewahrt wird.

3. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Schlüsselvereinbarungsabbildung k eine diskrete Exponentialfunktion modulo einer großen Primzahl p : $k(x,y) := x^y$ modulo p ist und daß der öffentliche Parameter g ein Element eines mathematischen Körpers $GF(p)$ von großer multiplikativer Ordnung ist.
4. Verfahren nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, daß die Schlüsselvereinbarungsabbildung k die Multiplikation auf einer elliptischen Kurve ist.
5. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß zur Wiederherstellung des Chiffrierschlüssels C im Verlustfalle seitens der Vertrauensstelle aus der Regenerierinformation R der Seed $S=k(R,v)$ berechnet wird.
6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Vertrauensstelle nach Berechnung des Seeds S und nach Ableitung des neuen öffentlichen Nutzerschlüssels U des Nutzers und des neuen Chiffrierschlüssels C aufgrund eines Schlüsselverlustes überprüft, ob der neu berechnete öffentliche Schlüssel U mit dem ursprünglichen öffentlichen Schlüssel U des Nutzers identisch ist, und den rekonstruierten Chiffrierschlüssel C nur dann an den Nutzer aushändigt, wenn dies zutrifft.
7. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß es mehrere Vertrauensstellen gibt, welche die Schlüsselvereinbarungsabbildung k und den öffentlichen Parameter g benutzen. Bei der Generierung des Chiffrierschlüssels C werden eine oder mehrere dieser Vertrauensstellen ausgewählt, wobei mit Hilfe jeder der

ausgewählten Vertrauensstellen ein anderer Teilwert S_v des Seeds nutzerseitig wie beschrieben erstellt und die Teilseeds S_v nutzerseitig zu dem Seed S verknüpft werden. Zur Regenerierung des Chiffrierschlüssels C im Verlustfalle wird von den ausgewählten Vertrauensstellen ihr jeweiliger Teilwert S_v des Seeds S mittels der Regenerierinformation R berechnet. Die rekonstruierten Teilwerte S_v werden zur Rekonstruktion des Chiffrierschlüssels C miteinander zu dem Seed S verknüpft.

8. Verfahren nach Anspruch 7, dadurch gekennzeichnet, daß die verschiedenen Vertrauensstellen verschiedene Funktionen k_v oder/und verschiedene öffentliche Parameter g_v benutzen und daß für jede der ausgewählten Vertrauensstellen eine eigene Regenerierinformation R_v erstellt wird.

THIS PAGE BLANK (USPTO)

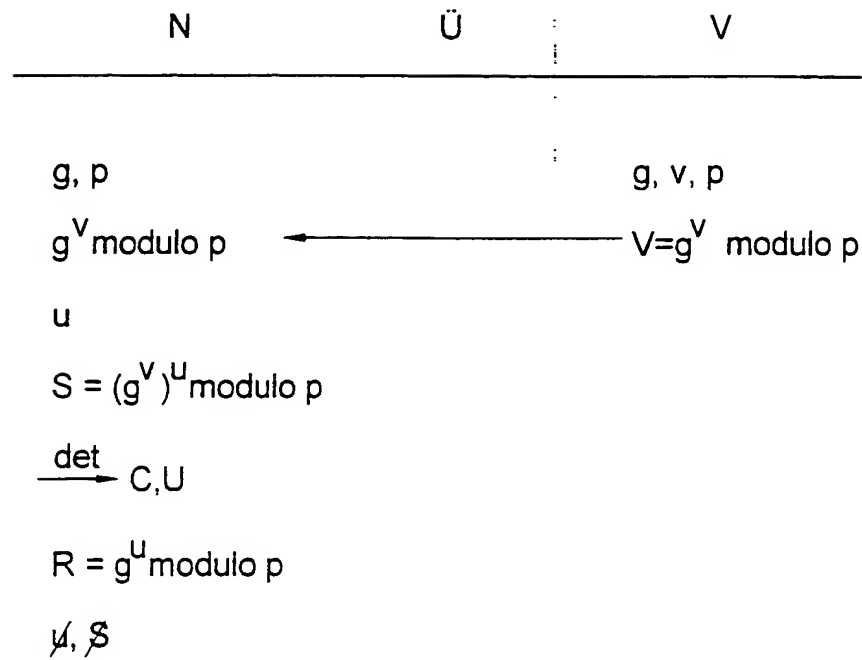


Fig. 1

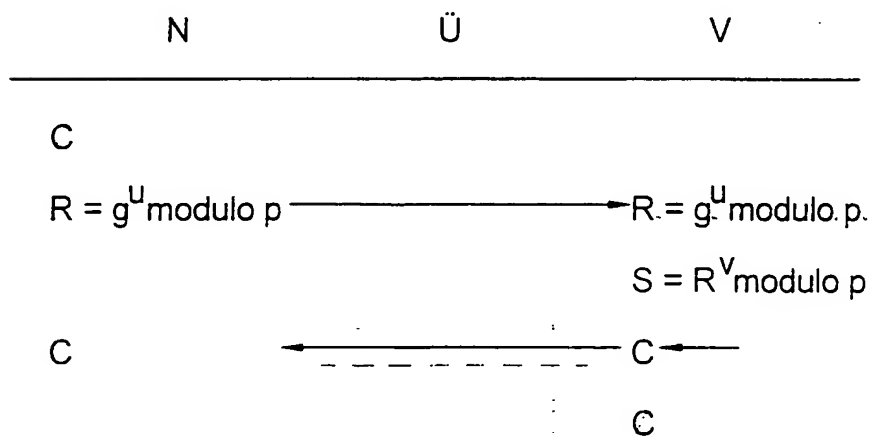


Fig. 2

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 00/06387

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, INSPEC, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	MAHER D P: "CRYPTOBACKUP AND KEY ESCROW" COMMUNICATIONS OF THE ASSOCIATION FOR COMPUTING MACHINERY, US, ASSOCIATION FOR COMPUTING MACHINERY. NEW YORK, vol. 39, no. 3, 1 March 1996 (1996-03-01), pages 48-53, XP000584954 ISSN: 0001-0782 page 50 -page 51	1-8
A	MENEZES A. J., VANSTONE S., VAN OORSCHOT P.: "Handbook of Applied Cryptography" 1997, CRC PRESS, USA XP002153673 ISBN: 0-8493-8523-7 page 130 page 524 -page 525	4, 8

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *G* document member of the same patent family

Date of the actual completion of the international search

23 November 2000

Date of mailing of the international search report

13/12/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Authorized officer

Carnerero Álvaro, F

THIS PAGE BLANK (USPTO)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 00/06387

A. KLASSTIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 H04L9/08

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, INSPEC, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	MAHER D P: "CRYPTOBACKUP AND KEY ESCROW" COMMUNICATIONS OF THE ASSOCIATION FOR COMPUTING MACHINERY, US, ASSOCIATION FOR COMPUTING MACHINERY. NEW YORK, Bd. 39, Nr. 3, 1. März 1996 (1996-03-01), Seiten 48-53, XP000584954 ISSN: 0001-0782 Seite 50 -Seite 51	1-8
A	MENEZES A. J., VANSTONE S., VAN OORSCHOT P.: "Handbook of Applied Cryptography" 1997, CRC PRESS, USA XP002153673 ISBN: 0-8493-8523-7 Seite 130 Seite 524 -Seite 525	4,8

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☐ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

A Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

E älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

L Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

O Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benützung, eine Ausstellung oder andere Maßnahmen bezieht

P Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

g Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

23. November 2000

Absenddatum des internationalen Recherchenberichts

13/12/2000

Name und Postanschrift der Internationalen Recherchenbehörde
Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-3016

Bevollmächtigter Bediensteter

Carnerero Álvaro, F

THIS PAGE BLANK (USPTO)

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P99075WO.1P	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/EP00/06387	International filing date (day/month/year) 06 July 2000 (06.07.00)	Priority date (day/month/year) 27 July 1999 (27.07.99)
International Patent Classification (IPC) or national classification and IPC H04L 9/08		
Applicant DEUTSCHE TELEKOM AG		

- This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.
- This REPORT consists of a total of 6 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).
 These annexes consist of a total of _____ sheets.

- This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand 11 January 2001 (11.01.01)	Date of completion of this report 07 December 2001 (07.12.2001)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

THIS PAGE BLANK (USPTO)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/EP00/06387

I. Basis of the report

1. With regard to the elements of the international application:*

- ☐ the international application as originally filed
- ☒ the description:
 pages 1-8, as originally filed
 pages _____, filed with the demand
 pages _____, filed with the letter of _____
- ☒ the claims:
 pages 1-8, as originally filed
 pages _____, as amended (together with any statement under Article 19
 pages _____, filed with the demand
 pages _____, filed with the letter of _____
- ☒ the drawings:
 pages 1/1, as originally filed
 pages _____, filed with the demand
 pages _____, filed with the letter of _____
- ☐ the sequence listing part of the description:
 pages _____, as originally filed
 pages _____, filed with the demand
 pages _____, filed with the letter of _____

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language _____ which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

THIS PAGE BLANK (USPTO)

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**1. Statement**

Novelty (N)	Claims		YES
	Claims	1	NO
Inventive step (IS)	Claims		YES
	Claims	1-8	NO
Industrial applicability (IA)	Claims	1-8	YES
	Claims		NO

2. Citations and explanations

Reference is made to the following documents:

D1: MAHER D.P.: 'CRYPTOBACKUP AND KEY ESCROW'
COMMUNICATIONS OF THE ASSOCIATION FOR COMPUTING
MACHINERY, US, ASSOCIATION FOR COMPUTING
MACHINERY. NEW YORK, Vol. 39, No. 3, 1 March
1996 (1996-03-01), pages 48-53, XP000584954
ISSN: 0001-0782

D2: MENEZES A.J., VANSTONE S., VAN OORSCHOT P.:
'Handbook of Applied Cryptography' 1997, CRC
PRESS, USA XP002153673, ISBN: 0-8493-8523-7.

1. Independent Claim 1

Document D1 (cf. in particular pages 50 to 51) discloses, as per all of the features of Claim 1, a method for generating/regenerating an encryption key for a cryptographic method, said encryption key being created from a large random number, seed S, using a predetermined deterministic method, characterised in that:

- the seed S ($f(y, r_u)$ - page 50, column 6, row 18) is only created by the user by using variables u (r_u - page 50, column 6, row 17) known only to the

THIS PAGE BLANK (USF14)

- user (page 50, columns 5 and 6),
- a regeneration information R ($f(x, r_u)$ - page 50, column 6, row 20) suitable for regenerating the seed and from which the seed can be derived deterministically by the confidence station by linking thereto information v (r_M - page 50, column 6, rows 6 and 7) known only to said confidence station is stored by the user in a loss-proof manner (page 50, columns 5 and 6), and
 - in the event of the encryption key C (k - page 50, column 6, row 18) being lost, the seed S can be recreated by the confidence station by linking the regeneration information R to the secret information v (page 50, columns 5 and 6).

Consequently, all of the features of Claim 1 are known from document D1.

The subject matter of Claim 1 is therefore not novel (PCT Article 33(2)).

Even if Claim 1 were amended such that there were no longer any objections with respect to novelty, it would not be admissible over the prior art since its subject matter lacks inventive step.

2. Dependent Claims 2 to 8

Dependent Claims 2 to 8 do not contain any features which, in combination with the features of any claim to which they refer, meet the PCT inventive step requirements. These claims contain known method features which are standard to a person skilled in the art and can also be derived from the citations D1 and D2.

THIS PAGE BLANK (USPTO)

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

1. Contrary to PCT Rule 5.1(a)(ii), the description does not cite documents D1 and D2 or indicate the relevant prior art disclosed therein.

THIS PAGE BLANK (USPTO)

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

In the preamble of Claim 1, the applicant discloses a method for generating/regenerating an encryption key for a cryptographic method, wherein the encryption key and a public key are produced from a large random number (seed) using a predetermined deterministic method.

Neither the characterising portion of Claim 1 nor the description discloses the technical features necessary for creating the two keys. Claim 1 only describes the reproduction of the seed, not how the encryption key and the corresponding public key are created from this seed.

Since Claim 1 does not contain essential technical features, it does not meet the requirements of PCT Article 6 in conjunction with PCT Rule 6.3(b).

2. The reference signs placed between parentheses in Claim 1 are definitions of the corresponding features and not reference signs. Only reference signs relating to the features of the claim may be placed between parentheses (PCT Rule 6.2(b)).

3. Dependent Claim 2 gives an explanation in parentheses: "(key specification mapping)". This addition cannot be interpreted as a reference sign (see PCT Rule 6.2(b)). However, since the addition refers indirectly to parts of the description (see, *inter alia*, the description, page 4), it is not in accordance with PCT Rule 6.2(a).

THIS PAGE BLANK (USPTO)

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

REC'D 11 DEC 2001

WIPO PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts 3084 FTZ PC 01	WEITERES VORGEHEN siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/EP00/06387	Internationales Anmeldedatum (Tag/Monat/Jahr) 06/07/2000	Prioritätsdatum (Tag/Monat/Tag) 27/07/1999
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK H04L9/08		
Anmelder DEUTSCHE TELEKOM AG et al.		



- Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
- Dieser BERICHT umfaßt insgesamt 6 Blätter einschließlich dieses Deckblatts.

☐ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

 Diese Anlagen umfassen insgesamt Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

- I ☒ Grundlage des Berichts
- II ☐ Priorität
- III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- IV ☐ Mangelnde Einheitlichkeit der Erfindung
- V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- VI ☐ Bestimmte angeführte Unterlagen
- VII ☒ Bestimmte Mängel der internationalen Anmeldung
- VIII ☒ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags 11/01/2001	Datum der Fertigstellung dieses Berichts 07.12.2001
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:  Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Apostolescu, R Tel. Nr. +49 89 2399 7950 

THIS PAGE BLANK (USPTO)

I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17)*):
Beschreibung, Seiten:

1-8 ursprüngliche Fassung

Patentansprüche, Nr.:

1-8 ursprüngliche Fassung

Zeichnungen, Blätter:

1/1 ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

THIS PAGE BLANK (USPTO)

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP00/06387

- ☐ Beschreibung, Seiten:
☐ Ansprüche, Nr.:
☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja: Ansprüche	
	Nein: Ansprüche	1
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	
	Nein: Ansprüche	1-8
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1-8
	Nein: Ansprüche	

2. Unterlagen und Erklärungen siehe Beiblatt

VII. Bestimmte Mängel der internationalen Anmeldung

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:
siehe Beiblatt

VIII. Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:
siehe Beiblatt

THIS PAGE BLANK (b)(1)

Zu Punkt V

Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

Es wird auf die folgenden Dokumente verwiesen:

- D1: MAHER D P: 'CRYPTOBACKUP AND KEY ESCROW' COMMUNICATIONS OF THE ASSOCIATION FOR COMPUTING MACHINERY,US,ASSOCIATION FOR COMPUTING MACHINERY. NEW YORK, Bd. 39, Nr. 3, 1. März 1996 (1996-03-01), Seiten 48-53, XP000584954 ISSN: 0001-0782
- D2: MENEZES A. J., VANSTONE S., VAN OORSCHOT P.: 'Handbook of Applied Cryptography' 1997 , CRC PRESS , USA XP002153673 ISBN: 0-8493-8523-7

1. Unabhängiger Anspruch 1.

Dokument D1 (vgl. insbes. Seite 50 bis 51) offenbart, gemäß allen Merkmalen des Anspruchs 1, ein Verfahren zur Generierung/Regenerierung eines Chiffrierschlüssels für ein Kryptographieverfahren, wobei der Chiffrierschlüssels mittels eines vorgegebenen deterministischen Verfahrens aus einer großen Zufallszahl, Seed S, erzeugt wird, dadurch gekennzeichnet,

- ◆ daß der Seed S ($f(y, r_U)$ - Seite 50, Spalte 6, Reihe 18) nur nutzerseitig durch Hinzuziehung von nur dem Nutzer bekannten Größen u (r_U - Seite 50, Spalte 6, Reihe 17) erzeugt wird (Seite 50, Spalte 5 und 6),
- ◆ daß eine zur Regenerierung des Seeds geeignete Regenerierinformation R ($f(x, r_U)$ - Seite 50, Spalte 6, Reihe 20), aus welcher der Seed von der Vertrauensstelle durch Verknüpfung mit nur ihr bekannten Information v (r_M - Seite 50, Spalte 6, Reihe 6 und 7) deterministisch ableitbar ist, nutzerseitig und verlustsicher aufbewahrt wird (Seite 50, Spalte 5 und 6) und
- ◆ daß im Falle eines Verlustes des Chiffrierschlüssels C (k - Seite 50, Spalte 6, Reihe 18) durch Verknüpfung der Regenerierinformation R mit den geheimen

THIS PAGE BLANK (USPTO)

Information v der Seed S seitens der Vertrauensstelle wieder hergestellt wird
(Seite 50, Spalte 5 und 6).

Alle Merkmale des Anspruchs 1 sind demnach aus Dokument D1 bekannt.

Der Gegenstand des Anspruchs 1 ist somit nicht neu (Artikel 33 (2) PCT).

Selbst wenn der Anspruch 1 dahingehend geändert würde, daß bezüglich der Neuheit keine Einwände mehr bestünden, so wäre er gegenüber dem Stand der Technik mangels erfinderischer Tätigkeit seines Gegenstandes nicht gewährbar.

2. Abhängige Ansprüche 2 bis 8.

Die abhängige Ansprüche 2 bis 8 enthalten keine Merkmale, die in Kombination mit den Merkmalen irgendeins Anspruchs, auf den sie sich beziehen, die Erfordernisse des PCT in bezug auf erfinderische Tätigkeit erfüllen.

Diese Ansprüche enthalten bekannte Verfahrensmaßnahmen, die dem Fachmann geläufig sind, und welche auch aus der Engegenhaltungen D1 und D2 zu entnehmen sind.

Zu Punkt VII

Bestimmte Mängel der internationalen Anmeldung

1. Im Widerspruch zu den Erfordernissen der Regel 5.1 a) ii) PCT werden in der Beschreibung weder der in den Dokumenten D1 und D2 offenbarte einschlägige Stand der Technik noch diese Dokumente angegeben.

Zu Punkt VIII

Bestimmte Bemerkungen zur internationalen Anmeldung

Die Anmelderin offenbart in dem Oberbegriff des Patentanspruchs 1 ein Verfahren zur Generierung/Regenerierung eines Chiffrierschlüssels für ein Kryptographieverfahren, wobei der Chiffrierschlüssel sowie ein öffentlicher Schlüssel mittels eines

THIS PAGE BLANK (USPTO)

vorgegebenen deterministischen Verfahrens aus einer großen Zufallszahl (Seed) erzeugt wird.

Weder in der charakteristischen Teil des Anspruchs 1 noch in der Beschreibung werden die technischen Merkmale offenbart, die zur Erzeugung der beiden Schlüsseln notwendig sind. In Anspruch 1 wird nur die Wiederherstellung des Seeds beschrieben, nicht aber auch wie man aus diesem Seed den Chiffrierschlüssel und den dazugehörenden öffentlicher Schlüssel erzeugt werden.

Da der Anspruch 1 wesentliche technische Merkmale nicht enthält, entspricht er nicht dem Erfordernis des Artikels 6 PCT in Verbindung mit Regel 6.3 (b) PCT.

2. Die im Anspruch 1 in Klammern gesetzten Zeichen sind Definitionen der entsprechenden Merkmale und nicht Bezugszeichen. Nur die Bezugszeichen der Merkmale der Ansprüche dürfen in Klammer gesetzt werden (Regel 6.2 (b) PCT)..

3. Der abhängige Anspruch 2 beinhaltet die Erläuterung im Klammern, wie "(Schlüsselvereinbarungsabbildung)". Diese Ergänzung kann nicht als Referenzzeichen (siehe Regel 6.2 (b) PCT) interpretiert werden. Da die Ergänzung sich aber indirekt auf Teile der Beschreibung bezieht (siehe u. a. Beschreibung Seite 4), steht sie nicht im Einklang mit den Auflagen der Regel 6.2 (a) PCT.

THIS PAGE BLANK (USP 10)

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts P99075W0.1P	WEITERES VORGEHEN siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
Internationales Aktenzeichen PCT/EP 00/ 06387	Internationales Anmeldedatum (Tag/Monat/Jahr) 06/07/2000	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) 27/07/1999
Anmelder DEUTSCHE TELEKOM AG		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.

☒ Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. Grundlage des Berichts

- a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

☐ Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

- b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

☐ in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

☐ Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. ☐ Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen (siehe Feld I).

3. ☐ Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 2

☐ wie vom Anmelder vorgeschlagen

☐ keine der Abb.

☒ weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

☐ weil diese Abbildung die Erfindung besser kennzeichnet.

THIS PAGE BLANK

A. KLASSTIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 7 H04L9/08

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 H04L

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, INSPEC, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	✓ MAHER D P: "CRYPTOBACKUP AND KEY ESCROW" COMMUNICATIONS OF THE ASSOCIATION FOR COMPUTING MACHINERY, US, ASSOCIATION FOR COMPUTING MACHINERY. NEW YORK, Bd. 39, Nr. 3, 1. März 1996 (1996-03-01), Seiten 48-53, XP000584954 ISSN: 0001-0782 Seite 50 -Seite 51	1-8
A	✓ MENEZES A. J., VANSTONE S., VAN OORSCHOT P.: "Handbook of Applied Cryptography" 1997, CRC PRESS, USA XP002153673 ISBN: 0-8493-8523-7 Seite 130 Seite 524 -Seite 525	4, 8



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

A Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

E älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

L Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

O Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

P Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

Z Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

23. November 2000

Absendedatum des internationalen Recherchenberichts

13/12/2000

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Carnerero Álvaro, F

THIS PAGE BLANK (USP14)

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 23(10)Gevas	FOR FURTHER ACTION see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/EP 00/ 02873	International filing date (day/month/year) 31/03/2000	(Earliest) Priority Date (day/month/year)
Applicant GEVAS VERPACKUNGSMASCHINEN GMBH		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 2 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

- a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.

☐ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

- b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing :

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. ☐ **Certain claims were found unsearchable** (See Box I).

3. ☐ **Unity of invention is lacking** (see Box II).

4. With regard to the **title**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

☒ the text is approved as submitted by the applicant.

☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No.

☒ as suggested by the applicant.

☐ because the applicant failed to suggest a figure.

☐ because this figure better characterizes the invention.

1
☐ None of the figures.

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 00/02873

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 B65H45/101

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 B65H B65D

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 98 58864 A (STAC PAC TECHNOLOGIES INC.) 30 December 1998 (1998-12-30) cited in the application page 5, paragraph 3 -page 6, paragraph 1 page 8, paragraph 3 -page 9, paragraph 3; figures 1,2 -----	1,9
A	US 6 009 689 A (O'CONNOR) 4 January 2000 (2000-01-04) column 7, line 60 -column 9, line 65; figures 5-8 -----	1,9
A	US 4 499 707 A (DESJOBERT ET AL) 19 February 1985 (1985-02-19) the whole document -----	1,9



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *&* document member of the same patent family

Date of the actual completion of the international search

5 December 2000

Date of mailing of the international search report

13/12/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Raven, P

THIS PAGE BLANK (USPTO)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 00/02873

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9858864 A	30-12-1998	US 6035608 A	14-03-2000
		US 5927051 A	27-07-1999
		US 5966905 A	19-10-1999
		US 6067775 A	30-05-2000
		US 6009689 A	04-01-2000
		US 5987851 A	23-11-1999
		AT 192117 T	15-05-2000
		AU 7902898 A	04-01-1999
		BR 9810162 A	08-08-2000
		CN 1260760 T	19-07-2000
		DE 19881126 T	23-09-1999
		DE 29823583 U	07-10-1999
		DE 29823901 U	31-08-2000
		DE 69800128 D	31-05-2000
		EP 0910542 A	28-04-1999
		ES 2148007 T	01-10-2000
		NO 996293 A	17-12-1999
		PL 337160 A	31-07-2000
		US 5956926 A	28-09-1999
		AU 3923599 A	06-12-1999
		WO 9959907 A	25-11-1999
US 6009689 A	04-01-2000	AT 192117 T	15-05-2000
		AU 7902898 A	04-01-1999
		BR 9810162 A	08-08-2000
		WO 9858864 A	30-12-1998
		CN 1260760 T	19-07-2000
		DE 19881126 T	23-09-1999
		DE 29823583 U	07-10-1999
		DE 29823901 U	31-08-2000
		DE 69800128 D	31-05-2000
		EP 0910542 A	28-04-1999
		ES 2148007 T	01-10-2000
		NO 996293 A	17-12-1999
		PL 337160 A	31-07-2000
US 4499707 A	19-02-1985	FR 2450776 A	03-10-1980
		AR 220819 A	28-11-1980
		BE 882145 A	08-09-1980
		BR 8001390 A	11-11-1980
		CA 1125243 A	08-06-1982
		CH 634531 A	15-02-1983
		DE 3008839 A	18-09-1980
		ES 489313 A	16-08-1980
		GB 2044304 A,B	15-10-1980
		GB 2065179 A	24-06-1981
		GB 2097026 A,B	27-10-1982
		IT 1141185 B	01-10-1986
		JP 55119664 A	13-09-1980
		LU 82232 A	24-09-1980
		NL 8000245 A	11-09-1980

THIS PAGE BLANK (USPTO)